

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号  
特開2002-312316  
(P2002-312316A)

(43)公開日 平成14年10月25日(2002.10.25)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード*(参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 A 5 B 0 8 5
13/00	5 1 0	13/00	5 1 0 S 5 J 1 0 4
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 E 5 K 0 3 0
H 0 4 L 9/32		H 0 4 L 12/22	
12/22		9/00	6 7 1

審査請求 未請求 請求項の数13 O L (全 11 頁)

(21)出願番号 特願2001-114891(P2001-114891)

(22)出願日 平成13年4月13日(2001.4.13)

(71)出願人 399104844  
住商情報システム株式会社  
東京都中央区晴海1丁目8番12号  
(72)発明者 加藤 道明  
東京都墨田区両国2丁目10番14号 住商情  
報システム株式会社内  
(74)代理人 100105784  
弁理士 橘 和之

最終頁に続く

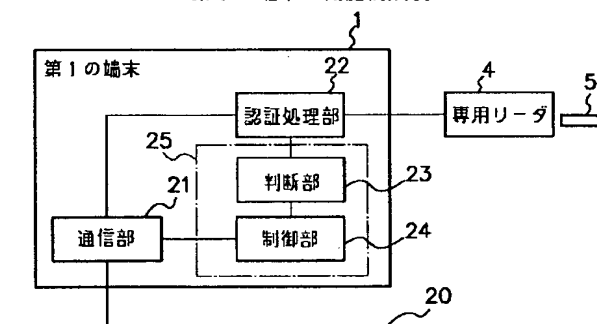
(54)【発明の名称】 不正アクセス防止装置および方法、不正アクセス防止用プログラム、記録媒体

(57)【要約】

【課題】 ユーザ認証が成立した端末を踏み台にして他人が正規利用者になりすますといった不正アクセスを有効に防止できるようにする。

【解決手段】 ネットワーク20上に接続された第1の端末1に関してユーザ認証が成立しているか否かを判断する判断部23と、ユーザ認証が成立している間は第1の端末1に対する外部からのアクセスを遮断する(例えば、外部から第1の端末1にアクセス要求が送られてきても応答を返さない)ように制御する制御部24とを設け、ユーザ認証が成立した第1の端末1が外部から見えないようにして当該端末1をハッキングできないようにし、これにより、ユーザ認証が成立した第1の端末1を踏み台に他人が正規利用者になりすまして目的のシステムに不正にアクセスすることを有効に防止する。

第1の端末の機能構成例



## 【特許請求の範囲】

【請求項1】 ネットワーク上に接続された端末に関して、上記ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証が成立しているか否かを判断する判断手段と、  
上記判断手段により上記ユーザ認証が成立していると判断された場合に、上記端末に対する外部からのアクセスを遮断するように制御する制御手段とを備えたことを特徴とする不正アクセス防止装置。

【請求項2】 ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証を受ける機能を備えた端末に適用する不正アクセス防止装置であって、  
上記ネットワークを介して外部から上記端末にアクセス要求が送られてきたときに、上記端末に関して上記ユーザ認証が成立しているか否かを判断する判断手段と、  
上記判断手段により上記ユーザ認証が成立していると判断された場合に、上記アクセス要求に対する応答を出力しないように制御する制御手段とを備えたことを特徴とする不正アクセス防止装置。

【請求項3】 上記制御手段は、上記端末に関して上記ユーザ認証が成立している間に、上記ユーザ認証によりアクセスが許可されたシステム以外の外部から上記ネットワークを介して上記端末にアクセス要求が送られてきたときに、上記アクセス要求に対する応答を出力しないように制御することを特徴とする請求項2に記載の不正アクセス防止装置。

【請求項4】 宛先アドレスをもとに経路情報を参照し、転送する次のノードを判断してデータ転送する機能を備えたネットワーク上の中継機器に適用する不正アクセス防止装置であって、  
上記ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証を受ける機能を備えた端末に関して、上記ユーザ認証が成立したか否かを判断する判断手段と、  
上記判断手段により上記ユーザ認証が成立したと判断されたときに、上記経路情報を退避させ、上記ユーザ認証が成立した端末を宛先とする経路を遮断した第2の経路情報に置き換えるとともに、上記判断手段により上記ユーザ認証が解除されたと判断されたときに、上記第2の経路情報を上記退避しておいた元の経路情報に戻すように制御する制御手段とを備えたことを特徴とする不正アクセス防止装置。

【請求項5】 上記第2の経路情報は、上記ユーザ認証によりアクセスが許可されたシステム以外の外部から上記端末を宛先とした経路を遮断するための経路情報であることを特徴とする請求項4に記載の不正アクセス防止装置。

【請求項6】 ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証を受

ける機能を備えた端末に外部から上記ネットワークを介してアクセス要求が送られてきたときに、上記端末に関して上記ユーザ認証が成立しているか否かを判断する第1のステップと、

上記端末に関して上記ユーザ認証が成立していると判断された場合に、上記アクセス要求に対する応答を出力しないように制御する第2のステップとを有することを特徴とする不正アクセス防止方法。

【請求項7】 上記第2のステップでは、上記端末に関して上記ユーザ認証が成立している間に、上記ユーザ認証によりアクセスが許可されたシステム以外の外部から上記ネットワークを介して上記端末にアクセス要求が送られてきたときに、上記アクセス要求に対する応答を出力しないように制御することを特徴とする請求項6に記載の不正アクセス防止方法。

【請求項8】 ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証を受ける機能を備えた端末に関して、上記ユーザ認証の成否を判断する第1のステップと、

上記端末に関して上記ユーザ認証が成立したときに、宛先アドレスをもとに経路情報を参照して次のノードにデータ転送する中継機器の上記経路情報を退避させ、上記ユーザ認証が成立した端末を宛先とする経路を遮断した第2の経路情報に置き換える第2のステップと、  
上記端末に関して上記ユーザ認証が解除されたときに、上記第2の経路情報を上記退避しておいた元の経路情報に戻す第3のステップとを有することを特徴とする不正アクセス防止方法。

【請求項9】 上記第2の経路情報は、上記ユーザ認証によりアクセスが許可されたシステム以外の外部から上記端末を宛先とした経路を遮断するための経路情報であることを特徴とする請求項8に記載の不正アクセス防止方法。

【請求項10】 ネットワーク上に接続された端末に関して、上記ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証が成立しているか否かを判断する判断手段、および上記判断手段により上記ユーザ認証が成立していると判断された場合に、上記端末に対する外部からのアクセスを遮断するように制御する制御手段としてコンピュータを機能させるための不正アクセス防止プログラム。

【請求項11】 ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証を受ける機能を備えた端末に外部から上記ネットワークを介してアクセス要求が送られてきたときに、上記端末に関して上記ユーザ認証が成立しているか否かを判断する判断手段、および上記判断手段により上記ユーザ認証が成立していると判断された場合に、上記アクセス要求に対する応答を出力しないように制御する制御手段としてコンピュータを機能させるための不正アクセス防止プロ

グラム。

【請求項12】 ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証を受ける機能を備えた端末に関して、上記ユーザ認証が成立したか否かを判断する判断手段、

上記判断手段により上記ユーザ認証が成立したと判断されたときに、宛先アドレスをもとに経路情報を参照して次のノードにデータ転送する中継機器の上記経路情報を退避させ、上記ユーザ認証が成立した端末を宛先とする経路を遮断した第2の経路情報に置き換える手段、および上記判断手段により上記ユーザ認証が解除されたと判断されたときに、上記第2の経路情報を上記退避しておいた元の経路情報に戻す手段としてコンピュータを機能させるための不正アクセス防止プログラム。

【請求項13】 請求項10～12の何れか1項に記載の各手段としてコンピュータを機能させるためのプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は不正アクセス防止装置および方法、不正アクセス防止用プログラム、記録媒体に関し、例えば、ネットワークもしくは当該ネットワーク上のシステムにアクセスするのに必要なユーザ認証を受ける機能を備えた端末や、宛先アドレスをもとに経路情報を参照し、転送する次のノードを判断してデータ転送する機能を備えたネットワーク上の中継機器に適用して好適なものである。

【0002】

【従来の技術】 近年、インターネットやイントラネットなどのネットワークを利用した情報システムが広く用いられている。この情報システムにおいては、他人による不正侵入、情報漏洩、改ざん、情報システム自体の稼働妨害などをいかに防ぐかが重要な課題となっている。情報システムの安全を守るためのセキュリティシステムとしては幾つかの技術が存在するが、その中の1つに、ユーザ認証技術がある。

【0003】 ユーザ認証技術の代表的なものは、パスワードである。すなわち、個々のユーザが自分に割り当てられた固有のパスワードをキーボードなどから入力し、そのパスワードが個人認証システムにより照合されて正しいことが確かめられると、ネットワークや当該システム上のシステムへのアクセスができるようになるものである。

【0004】 ところが、近年においてはハッキング技術が向上し、パスワードを盗むことは簡単になってきている。そのため、パスワードによるユーザ認証では、他人による不正アクセスを完全に防止することは事実上不可能であった。そこで最近では、解読が困難なICカードを利用したユーザ認証技術も用いられるようになってき

ている。しかし、このICカードを用いても、そのICカード自体が盗まれてしまうと、他人が正規利用者になりすまして不正にアクセスする恐れがあった。

【0005】 このような実情から、特に最近では、指紋や声、顔などを使って個人を識別する、いわゆるバイOMETRICS認証技術が注目され、開発されている。また、これとICカードとを組み合わせた技術も開発されている。例えば、ユーザの指紋データをICカードに格納しておき、ネットワーク等の利用時にそのICカードを端末に挿入してユーザ本人の指紋データとを照合し、正しければネットワーク等へのアクセスを許可するようにしたものである。

【0006】

【発明が解決しようとする課題】 上述のバイOMETRICS認証技術や、これとICカードとを組み合わせたユーザ認証技術などによれば、従来のパスワードやICカードを単体で用いる場合に比べて、情報システムの安全性を高めることが可能である。しかしながら、ユーザ認証技術をいかに駆使しても、ユーザ認証の成立した端末がハッキングされると、その端末を踏み台にして他人による不正なアクセスが行われてしまうという問題があった。

【0007】 このことを、図8を用いて詳しく説明する。図8に示すシステムでは、第1、第2の端末101、102と、人事・給与サーバ106とがネットワーク110を介して接続されている。人事・給与サーバ106にはデータベース107が接続されており、人事・給与に関する各種データが格納されている。この各種データの中には、個人の学歴・懲罰・病歴・健康状態・給与などに関する個人情報も含まれている。

【0008】 第1、第2の端末101、102と人事・給与サーバ106との間には、個人認証装置105が設置されている。個人認証装置105は、データベース107上のデータが改ざんされたり、個人情報が盗まれたりするといった不都合を回避すべく、人事・給与サーバ106に対するアクセスを特定のユーザに対してのみ許可するために、ユーザ認証に関する処理を行うものである。

【0009】 第1の端末101には、ICカード104の専用リーダ103が接続される。ICカード104には、人事・給与サーバ106に対するアクセス権を有するユーザに関する認証情報（ユーザのステータス情報、あるいは指紋などのバイオ情報等）を格納しておく。

【0010】 第1の端末101のユーザがネットワーク110を介して人事・給与サーバ106にアクセスする場合は、まず、ICカード104を専用リーダ103に挿入して自分の認証情報を第1の端末101に読み取らせる。第1の端末101は、読み取った認証情報を個人認証装置105に送る。個人認証装置105は、第1の端末101から送られてきた認証情報を確認し、正しけ

れば人事・給与サーバ106へのアクセスを許可する。

【0011】このようにして第1の端末101にユーザ認証が成立すると、当該第1の端末101から個人認証装置105を介して人事・給与サーバ106に至るパスが形成される。この状態で、第2の端末102から第1の端末101がハッキングされると、第1の端末101を踏み台にして第2の端末102のユーザが第1の端末1のユーザになりすまし、人事・給与サーバ106に不正にアクセスすることが可能となってしまう。

【0012】このように、従来は、ユーザ認証技術自体は改良が加えられ、正規利用者以外の他人がユーザ認証を受けることは困難になってきている。しかし、正規利用者によってユーザ認証の成立した端末をハッキングすることにより、当該端末を踏み台にして他人が正規利用者になりすますることが可能となってしまう。そのため、ネットワークや当該ネットワーク上のシステムに対する他人による不正アクセスを完全に防ぐことはできなかった。

【0013】本発明は、このような問題を解決するために成されたものであり、ユーザ認証が成立した端末を踏み台にして他人が正規利用者になりすましといった不正アクセスを有効に防止できるようにすることを目的とする。

#### 【0014】

【課題を解決するための手段】本発明の不正アクセス防止装置は、ネットワーク上に接続された端末に関して、上記ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証が成立しているか否かを判断する判断手段と、上記判断手段により上記ユーザ認証が成立していると判断された場合に、上記端末に対する外部からのアクセスを遮断するように制御する制御手段とを備えたことを特徴とする。

【0015】本発明の他の態様では、ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証を受ける機能を備えた端末に適用する不正アクセス防止装置であって、上記ネットワークを介して外部から上記端末にアクセス要求が送られてきたときに、上記端末に関して上記ユーザ認証が成立しているか否かを判断する判断手段と、上記判断手段により上記ユーザ認証が成立していると判断された場合に、上記アクセス要求に対する応答を出力しないように制御する制御手段とを備えたことを特徴とする。

【0016】本発明のその他の態様では、上記制御手段は、上記端末に関して上記ユーザ認証が成立している間に、上記ユーザ認証によりアクセスが許可されたシステム以外の外部から上記ネットワークを介して上記端末にアクセス要求が送られてきたときに、上記アクセス要求に対する応答を出力しないように制御することを特徴とする。

【0017】本発明のその他の態様では、宛先アドレス

をもとに経路情報を参照し、転送する次のノードを判断してデータ転送する機能を備えたネットワーク上の中継機器に適用する不正アクセス防止装置であって、上記ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証を受ける機能を備えた端末に関して、上記ユーザ認証が成立したか否かを判断する判断手段と、上記判断手段により上記ユーザ認証が成立したと判断されたときに、上記経路情報を退避させ、上記ユーザ認証が成立した端末を宛先とする経路を遮断した第2の経路情報に置き換えるとともに、上記判断手段により上記ユーザ認証が解除されたと判断されたときに、上記第2の経路情報を上記退避しておいた元の経路情報に戻すように制御する制御手段とを備えたことを特徴とする。

【0018】本発明のその他の態様では、上記第2の経路情報は、上記ユーザ認証によりアクセスが許可されたシステム以外の外部から上記端末を宛先とした経路を遮断するための経路情報であることを特徴とする。

【0019】また、本発明の不正アクセス防止方法は、ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証を受ける機能を備えた端末に外部から上記ネットワークを介してアクセス要求が送られてきたときに、上記端末に関して上記ユーザ認証が成立しているか否かを判断する第1のステップと、上記端末に関して上記ユーザ認証が成立していると判断された場合に、上記アクセス要求に対する応答を出力しないように制御する第2のステップとを有することを特徴とする。

【0020】本発明の他の態様では、上記第2のステップでは、上記端末に関して上記ユーザ認証が成立している間に、上記ユーザ認証によりアクセスが許可されたシステム以外の外部から上記ネットワークを介して上記端末にアクセス要求が送られてきたときに、上記アクセス要求に対する応答を出力しないように制御することを特徴とする。

【0021】本発明のその他の態様では、ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証を受ける機能を備えた端末に関して、上記ユーザ認証の成否を判断する第1のステップと、上記端末に関して上記ユーザ認証が成立したときに、宛先アドレスをもとに経路情報を参照して次のノードにデータ転送する中継機器の上記経路情報を退避させ、上記ユーザ認証が成立した端末を宛先とする経路を遮断した第2の経路情報に置き換える第2のステップと、上記端末に関して上記ユーザ認証が解除されたときに、上記第2の経路情報を上記退避しておいた元の経路情報に戻す第3のステップとを有することを特徴とする。

【0022】本発明のその他の態様では、上記第2の経路情報は、上記ユーザ認証によりアクセスが許可された

10

20

30

40

50

システム以外の外部から上記端末を宛先とした経路を遮断するための経路情報であることを特徴とする。

【0023】また、本発明の不正アクセス防止プログラムは、ネットワーク上に接続された端末に関して、上記ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証が成立しているか否かを判断する判断手段、および上記判断手段により上記ユーザ認証が成立していると判断された場合に、上記端末に対する外部からのアクセスを遮断するように制御する制御手段としてコンピュータを機能させるためのもの

である。  
【0024】本発明の他の態様では、ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証を受ける機能を備えた端末に外部から上記ネットワークを介してアクセス要求が送られてきたときに、上記端末に関して上記ユーザ認証が成立しているか否かを判断する判断手段、および上記判断手段により上記ユーザ認証が成立していると判断された場合に、上記アクセス要求に対する応答を出力しないように制御する制御手段としてコンピュータを機能させることを特徴とする。

【0025】本発明のその他の態様では、ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証を受ける機能を備えた端末に関して、上記ユーザ認証が成立したか否かを判断する判断手段、上記判断手段により上記ユーザ認証が成立したと判断されたときに、宛先アドレスをもとに経路情報を参照して次のノードにデータ転送する中継機器の上記経路情報を回避させ、上記ユーザ認証が成立した端末を宛先とする経路を遮断した第2の経路情報に置き換える手段、および上記判断手段により上記ユーザ認証が解除されたと判断されたときに、上記第2の経路情報を上記回避しておいた元の経路情報に戻す手段としてコンピュータを機能させることを特徴とする。

【0026】また、本発明のコンピュータ読み取り可能な記録媒体は、請求項10～12の何れか1項に記載の各手段としてコンピュータを機能させるためのプログラムを記録したことを特徴とする。

【0027】

【発明の実施の形態】（第1の実施形態）以下、本発明の第1の実施形態を図面に基づいて説明する。図1は、本実施形態による不正アクセス防止装置を適用したネットワークシステム全体の構成を示す図である。

【0028】図1において、1、2、3はパーソナルコンピュータ等から成る端末、9はファイルサーバ、10はメールサーバ、11は人事・給与サーバ、12は経理・財務サーバであり、これらがネットワーク20を介して互いに通信可能なように接続されている。

【0029】ファイルサーバ9は、ファイルの転送、削除、ディレクトリ操作などの処理を行う。メールサーバ

10は、端末1、2、3からの要求に基づいて電子メールを送信したり、届いた電子メールを保管して端末1、2、3からの照会があったときに引き渡したりする処理を行う。人事・給与サーバ11は、企業内の人事・給与に関する様々な処理を行う。経理・財務サーバ12は、企業内の経理・財務に関する様々な処理を行う。なお、これらの各種サーバ9～12は公知のものをを用いることが可能であるので、ここでは処理内容の詳細な説明は割愛する。

【0030】8はルータであり、ネットワーク20上の適当な位置に設置されている。あるコンピュータからネットワーク20上に送信されたデータは、必ずルータ8を経由して目的とするコンピュータに届けられる。このルータ8は、IPヘッダにある宛先IPアドレスをもとに、ルータ8自身が持つ経路情報（ルーティングテーブル）を参照し、転送する次のノードを判断してデータを転送する。

【0031】13は個人認証装置であり、第1～第3の端末1～3と、人事・給与サーバ11および経理・財務サーバ12との間に設置されている。個人認証装置13は、人事・給与サーバ11、経理・財務サーバ12に対するアクセスを特定のユーザに対してのみ許可するために、第1および第2の端末1、2から送られてくる認証情報に基づいてユーザ認証に関する処理を行う。

【0032】第1の端末1には、ICカード5の専用リーダ4が接続される。ICカード5には、例えば人事・給与サーバ11に対するアクセス権を有するユーザに関する認証情報（ユーザのステータス情報、あるいは指紋などのバイオ情報等）を格納しておく。第1の端末1のユーザは、ファイルサーバ9とメールサーバ10とに自由にアクセスすることができるとともに、ICカード5を用いてユーザ認証を受けることで、人事・給与サーバ11にもアクセスできるようになる。

【0033】第1の端末1のユーザが人事・給与サーバ11にアクセスする場合は、まず、ICカード5を専用リーダ4に挿入して自分の認証情報を第1の端末1に読み取らせる。第1の端末1は、読み取った認証情報をルータ8を介して個人認証装置13に送る。個人認証装置13は、第1の端末1から送られてきた認証情報を確認し、正しければ人事・給与サーバ11へのアクセスを許可する。

【0034】また、第2の端末2には、ICカード7の専用リーダ6が接続される。ICカード7には、例えば経理・財務サーバ12に対するアクセス権を有するユーザに関する認証情報（ユーザのステータス情報、あるいは指紋などのバイオ情報等）を格納しておく。第2の端末2のユーザは、ファイルサーバ9とメールサーバ10とに自由にアクセスすることができるとともに、ICカード7を用いてユーザ認証を受けることで、経理・財務サーバ12にもアクセスできるようになる。

【0035】第2の端末2のユーザが経理・財務サーバ12にアクセスする場合は、まず、ICカード7を専用リーダ6に挿入して自分の認証情報を第2の端末2に読み取らせる。第2の端末2は、読み取った認証情報をルータ8を介して個人認証装置13に送る。個人認証装置13は、第2の端末2から送られてきた認証情報を確認し、正しければ経理・財務サーバ12へのアクセスを許可する。

【0036】第3の端末3は、ユーザ認証を受けるための機能を備えていない。すなわち、第3の端末3のユーザは、人事・給与サーバ11および経理・財務サーバ12に対するアクセス権を持っておらず、ファイルサーバ9とメールサーバ10に対してのみアクセスすることが可能である。

【0037】なお、ここでは第1および第2の端末1、2の外付けでICカード5、7の専用リーダ4、6を設ける構成としたが、第1および第2の端末1、2自体がICカード5、7の読み取り機能を備えていても良い。また、ここではユーザ認証を受けるためにICカード5、7を用いているが、本発明はユーザ認証の方法は特

20 限しない。例えば、パスワードなどの他のユーザ認証技術を用いても良い。

【0038】また、ここでは、アクセスするのにユーザ認証を必要とするものを人事・給与サーバ11および経理・財務サーバ12としたが、これらのサーバに限定されるものではない。例えば、図示しない他のサーバもしくはファイルサーバ9やメールサーバ10、または図示しないホストコンピュータなどについても、個人認証装置13によるユーザ認証をアクセスの前提条件とするようにしても良い。

【0039】図2は、第1の端末1の機能構成例を示すブロック図である。なお、第2の端末2も第1の端末1と同様に構成されるので、ここでは図示を省略する。図2において、21は通信部であり、ネットワーク20を介してデータの送受信に関する処理を行う。22は認証処理部であり、個人認証装置13と共動してユーザ認証に関する処理を行う。

【0040】上記認証処理部22は、専用リーダ4にて読み取ったICカード5内の認証情報を取り込み、通信部21を介して個人認証装置13に送信する機能を有している。また、個人認証装置13から通信部21を介して送られてくる認証許可情報を取り込み、保持する機能も有している。認証処理部22が認証許可情報を保持している間だけ、人事・給与サーバ11にアクセスすることが可能である。

【0041】23は判断部であり、外部からネットワーク20を介して通信部21にアクセス要求が送られてきたときに、認証処理部22により認証許可情報が保持されているかどうかを見ることによって、第1の端末1に

【0042】なお、ここでは認証処理部22に認証許可情報を保持させ、当該情報の有無によってユーザ認証の成否を判断しているが、本発明はこの例に限定されるものではない。例えば、外部からアクセス要求が送られてきたときに、通信部21を介して個人認証装置13にユーザ認証の成否を問い合わせるようにしても良い。この場合は、個人認証装置13が認証許可情報を保持することになる。

【0043】24は制御部であり、第1の端末1に関してユーザ認証が成立している間に、外部からネットワーク20を介して第1の端末1にアクセス要求が送られてきたときは、そのアクセス要求に対する応答を通信部21から出力しないように制御する。一方、第1の端末1に関してユーザ認証が成立していないときは、通常通り、外部からのアクセス要求に対して応答を出力するように制御する。

【0044】上記判断部23および制御部24によって、本実施形態の不正アクセス防止装置25が構成される。この不正アクセス防止装置25は、実際には第1の端末1のCPUあるいはMPU、RAM、ROMなどで構成され、RAMやROMに記憶されたプログラムが動作することによって上述した判断部23および制御部24の機能構成が実現される。

【0045】したがって、第1の端末1が上記判断部23および制御部24の機能を果たすように動作させるプログラムを例えばCD-ROMのような記録媒体に記録し、コンピュータに読み込ませることによって実現できるものである。上記プログラムを記録する記録媒体としては、CD-ROM以外に、フロッピー（登録商標）ディスク、ハードディスク、磁気テープ、光ディスク、光磁気ディスク、DVD、不揮発性メモリカード等を用いることができる。また、上記プログラムをネットワーク20を介して他のコンピュータからダウンロードするようにしても良い。

【0046】また、第1の端末1が供給されたプログラムを実行することにより判断部23および制御部24の機能が実現されるだけでなく、そのプログラムが第1の端末1において稼働しているOS（オペレーティングシステム）あるいは他のアプリケーションソフト等と共同して上述の機能が実現される場合や、供給されたプログラムの処理の全てあるいは一部が第1の端末1の機能拡張ボードや機能拡張ユニットにより行われて上述の機能が実現される場合も、かかるプログラムは本発明の実施形態に含まれる。

【0047】図3は、一般的な通信プロトコルを示す図である。送信側から受信側にデータを送信する場合は、まず、送信側から受信側にデータ送信を開始することを伝える信号STARTを送る。これに対応して受信側から送信側に応答信号Ackが返されると、送信側から受信側にデータDataが送られる。データ送信が終了す

ると、送信側から受信側にデータ送信が終了したことを伝える信号ENDを送る。これに対応して受信側から送信側に応答信号Ackを返すことにより、一連のデータ通信が完了する。

【0048】このような通信プロトコルにおいて、制御部24は、第1の端末1に関してユーザ認証が成立している間に、アクセス要求であるデータ送信開始信号STARTが外部から送られてきたときは、それに対する応答信号Ackを返さないように制御する。このようにすることで、アクセス要求元に対して、第1の端末1はあ

たかもネットワーク20上に存在していないように見せることが可能となる。

【0049】通常、ユーザ認証が成立している第1の端末1に対するハッキングは、外部から第1の端末1に仮のデータを送るなどして、第1の端末1のネットワーク20上における存在位置を確認することによって行われる。しかし、本実施形態によれば、第1の端末1は、ユーザ認証が成立している間は外部からのアクセス要求に対して応答を返さないで、外部から第1の端末1の存在を知ることはできず、第1の端末1にアクセスすることは一切できなくなる。

【0050】したがって、例えば第3の端末3からユーザ認証が成立した第1の端末1をハッキングすることは全くできなくなり、第1の端末1を踏み台にして他人が第1の端末1のユーザになりすますことによる人事・給与サーバ11への不正アクセスを有効に防止することができる。同様に、ユーザ認証が成立した第2の端末2をハッキングすることもできなくなり、第2の端末2を踏み台にした経理・財務サーバ12への不正アクセスも有効に防止することができる。

【0051】以上の例では、例えば第1の端末1に関してユーザ認証が成立している間は、第1の端末1から人事・給与サーバ11にアクセスすることは可能であるが、逆に人事・給与サーバ11から第1の端末1にアクセスすることはできなくなる。しかし、例えば夜間にタイマをセットして、人事・給与サーバ11から起動して第1の端末1に所望のデータを送って印刷をするといった要求も存在する。

【0052】このような要求に対応するために、第1の端末1に関してユーザ認証が成立している間でも、ユーザ認証によりアクセスが許可された人事・給与サーバ11からのアクセスだけは許可する（応答信号Ackを返す）ようにすることも可能である。すなわち、この場合の制御部24は、人事・給与サーバ11以外のコンピュータからネットワーク20を介して第1の端末1にアクセス要求が送られてきたときに、そのアクセス要求に対する応答を出力しないように制御する。

【0053】図4は、この場合の第1の端末1に備えられる不正アクセス防止装置25の動作を示すフローチャートである。図4において、制御部24は、通信部21

が外部からデータ送信開始信号STARTを受信したかどうかを監視し（ステップS1）、これを受信した場合には、判断部23を用いて、現在第1の端末1に関してユーザ認証が成立しているかどうかを判定する（ステップS2）。

【0054】現在ユーザ認証が成立していない場合は、たとえ第1の端末1がハッキングされても、当該第1の端末1を踏み台にして人事・給与サーバ11にアクセスすることは不可能であるから、通常通り応答信号Ackを返すように通信部21を制御する（ステップS5）。これにより、第1の端末1に対して外部から自由にアクセスすることが可能となる。

【0055】一方、現在ユーザ認証が成立している場合には、制御部24は、アクセス要求元（データ送信開始信号STARTの発信元）が人事・給与サーバ11であるかどうかを判定する（ステップS3）。本実施形態のようにICカード5を使ってユーザ認証を行う場合、そのICカード5に認証情報を設定する上で、人事・給与サーバ11のIPアドレスも保持される。したがって、ICカード5から読み取ったIPアドレスと、データ送信開始信号STARTと共に送られてくるIPアドレスとが一致するかどうかを見ることによって、アクセス要求元が人事・給与サーバ11であるかどうかを判定することが可能である。

【0056】アクセス要求元が人事・給与サーバ11でなかった場合は、制御部24は、データ送信開始信号STARTに対して応答信号Ackを返さないように通信部21を制御する（ステップS4）。これにより、第1の端末1が外部から見えないようにし、第1の端末1を踏み台にした人事・給与サーバ11への不正アクセスを防止する。

【0057】また、アクセス要求元が人事・給与サーバ11であった場合は、制御部24は、データ送信開始信号STARTに対して応答信号Ackを返すように通信部21を制御する（ステップS5）。これにより、第1の端末1に対して人事・給与サーバ11から自由にアクセスすることが可能となる。

【0058】以上詳しく説明したように、第1の実施形態においては、第1および第2の端末1、2に関してユーザ認証が成立している間は、これらの端末1、2に対する外部からのアクセスを遮断するように制御しているので、第1および第2の端末1、2をハッキングすることができないようにすることができる。これにより、第1および第2の端末1、2を踏み台にして他人が個人認証装置13を通過し、人事・給与サーバ11や経理・財務サーバ12などに不正にアクセスすることを有効に防止することができる。

【0059】（第2の実施形態）次に、本発明の第2の実施形態を図面に基づいて説明する。第2の実施形態による不正アクセス防止装置を適用したネットワークシス

10

20

30

40

50

テム全体の構成は、図1と同様である。ただし、第1および第2の端末1, 2は、図2に示した不正アクセス防止装置25の機能構成を備えていない。本実施形態において不正アクセス防止装置は、ルータ8内に設けられる。

【0060】図5は、ルータ8の機能構成例を示すブロック図である。図5において、31は通信部であり、ネットワーク20を介してデータ転送に関する処理を行う。すなわち、ネットワーク20を介して送られてきたデータのIPヘッダにある宛先IPアドレスをもとに、経路情報メモリ35に保持されている経路情報（ルーティングテーブル）を参照し、転送する次のノードを判断してデータを転送する。

【0061】32は判断部であり、第1の端末1および第2の端末2に関するユーザ認証の成否を判断する。第1および第2の端末1, 2でユーザ認証を受ける場合は、これらの端末1, 2と個人認証装置13との間で、ルータ8を経由してユーザ認証に必要なデータがやり取りされる。したがって、ユーザ認証の実行の際にルータ8の通信部31を介してやり取りされるデータを判断部32が監視することによって、ユーザ認証が成立したことや、その後ユーザ認証が解除されたことを確認することが可能である。

【0062】なお、第1および第2の端末1, 2に関するユーザ認証の成否を判断する手法は、これに限定されない。例えば、第1および第2の端末1, 2でユーザ認証が成立もしくは解除されたときに、そのことを第1および第2の端末1, 2からルータ8に明示的に伝えるようにしても良い。

【0063】33は制御部であり、判断部32により第1の端末1あるいは第2の端末2に関してユーザ認証が成立したと判断されたときに、経路情報メモリ35内の経路情報を退避メモリ36に退避させ、ユーザ認証が成立した端末を宛先とする経路を遮断した第2の経路情報に、経路情報メモリ35の内容を置き換える。また、ユーザ認証が解除されたと判断されたときに、退避メモリ36に退避しておいた元の経路情報を経路情報メモリ35に戻すように制御する。

【0064】上記判断部32および制御部33によって、本実施形態の不正アクセス防止装置34が構成される。この不正アクセス防止装置34は、実際にはルータ8のCPUあるいはMPU、RAM、ROMなどで構成され、RAMやROMに記憶されたプログラムが動作することによって上述した判断部32および制御部33の機能構成が実現される。

【0065】図6は、経路情報の置き換え例を示す図である。図6(a)は、経路情報メモリ35に元々記憶されている経路情報（ルーティングテーブル）をイメージ的に示したものである。テーブル中の○印は、経路が存在することを示している。通常は、ネットワーク20上

に接続されている各ノードに関する全ての経路が○印となっている。

【0066】なお、第1の端末1から人事・給与サーバ11に対する経路、第2の端末2から経理・財務サーバ12に対する経路で“IC”と書かれているのは、ICカード5, 7を用いてユーザ認証を受けた場合にアクセスが許可される経路であることを示している。また、他のノードから人事・給与サーバ11や経理・財務サーバ12に対する経路も○印となっているが、これは単にそういう経路があるということを示しているだけで、アクセスを許可していることを意味するものではない。

【0067】例えば、第1の端末1に関してユーザ認証が成立したとする。この場合は、第1の端末1が受信側となる部分の経路情報を図6(b)のように置き換える。図6(b)中の×印は、そのような経路が存在しないことを意味するものである。この置き換えは、他のノードから第1の端末1に至る経路情報を全て破棄することに相当する。この置き換えをするとき、元の経路情報を後から復元できるようにするために、置き換える前の経路情報を退避メモリ36に退避させる。

【0068】その後、第1の端末1においてICカード5を抜くなどしてユーザ認証が解除されると、退避メモリ36に退避しておいた元の経路情報を経路情報メモリ35に戻すことにより、図6(a)の状態を復元する。なお、ユーザ認証の成立時に退避メモリ36に退避させる経路情報は、図6(a)に示す経路情報全てであっても良いし、置き換える部分のみであっても良い。

【0069】このように、第1の端末1に関してユーザ認証が成立している間は、他のノードから第1の端末1に至る経路の経路情報にマスクをかけることにより、アクセス要求元に対して、第1の端末1はあたかもネットワーク20上に存在していないように見せることが可能となる。第1の端末1にアクセスする際には必ずルータ8を経由するが、ユーザ認証成立時にはそのルータ8内の経路情報を置き換えているので、外部から第1の端末1の存在を知ることとはできず、第1の端末1にアクセスすることは一切できなくなる。

【0070】したがって、例えば第3の端末3からユーザ認証が成立した第1の端末1をハッキングすることは全くできなくなり、第1の端末1を踏み台にして他人が第1の端末1のユーザになりすますことによる人事・給与サーバ11への不正アクセスを有効に防止することができる。同様に、ユーザ認証が成立した第2の端末2をハッキングすることもできなくなり、第2の端末2を踏み台にした経理・財務サーバ12への不正アクセスも有効に防止することができる。

【0071】なお、第2の実施形態においても、例えば第1の端末1に関してユーザ認証が成立している間でも、ユーザ認証によりアクセスが許可された人事・給与サーバ11からのアクセスだけは許可する（人事・給与



サーバ11から第1の端末1に至る経路の経路情報はマスクしない)ようにすることも可能である。すなわち、図6.(b)の例で、下から2番目の部分は○印とする。

【0072】図7は、第2の実施形態による不正アクセス防止装置34の動作を示すフローチャートである。図7において、ルータ8内の制御部33は、判断部32を用いて、第1の端末1および第2の端末2に関してユーザ認証の成否(ユーザ認証の成立および解除)を監視している(ステップS11)。

【0073】第1の端末1および第2の端末2の双方ともユーザ認証が成立していない場合は、たとえこれらの端末1,2がハッキングされても、当該端末1,2を踏み台にして人事・給与サーバ11や経理・財務サーバ12にアクセスすることは不可能であるから、通常の経路情報を経路情報メモリ35にそのまま保持し、ユーザ認証の成否を監視し続ける。これにより、第1の端末1および第2の端末2に対して外部から自由にアクセスすることが可能である。

【0074】第1の端末1または第2の端末2に関してユーザ認証の成否に変化があったときは、それがユーザ認証の成立かどうかを判定する(ステップS12)。第1の端末1または第2の端末2にユーザ認証が成立した場合には、そのユーザ認証が成立した端末に関する経路情報を経路情報メモリ35から退避メモリ36に退避し、当該端末に至る経路をマスクした第2の経路情報を経路情報メモリ35に置き換える(ステップS13)。

【0075】一方、第1の端末1または第2の端末2に関してユーザ認証が解除された場合には、そのユーザ認証が解除された端末に関する経路情報を退避メモリ36から経路情報メモリ35に復元する(ステップS14)。上記ステップS13あるいはステップS14の処理の後、ステップS11に戻ってユーザ認証成否の監視を継続する。

【0076】以上詳しく説明したように、第2の実施形態においても、第1および第2の端末1,2に関してユーザ認証が成立している間は、これらの端末1,2に対する外部からのアクセスを遮断するように制御しているので、第1および第2の端末1,2をハッキングすることができないようにすることができる。これにより、第1および第2の端末1,2を踏み台にして他人が個人認証装置13を通過し、人事・給与サーバ11や経理・財務サーバ12などに不正にアクセスすることを有効に防止することができる。

【0077】なお、以上に説明した各実施形態は、何れも本発明を実施するにあたっての具体化の一例を示したものに過ぎず、これらによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその精神、またはその主要な特徴から逸脱することなく、様々な形で実施することができる。例えば、第1の実施形態と第2の実施形態とを組み合わせ適用し

ても良い。

【0078】

【発明の効果】本発明は上述したように、ネットワーク上に接続された端末に関してユーザ認証が成立している間は、そのユーザ認証が成立した端末に対する外部からのアクセスを遮断するように制御しているので、ユーザ認証が成立した端末をハッキングすることができないようにすることができる。これにより、ユーザ認証が成立した端末を踏み台に他人が正規利用者になりすまして目的のネットワークやシステムに不正にアクセスすることを有効に防止することができる。

【図面の簡単な説明】

【図1】第1および第2の実施形態による不正アクセス防止装置を適用したネットワークシステム全体の構成を示す図である。

【図2】第1の実施形態による第1の端末の機能構成例を示すブロック図である。

【図3】一般的な通信プロトコルを示す図である。

【図4】第1の実施形態による第1の端末に備えられる不正アクセス防止装置の動作を示すフローチャートである。

【図5】第2の実施形態によるルータの機能構成例を示すブロック図である。

【図6】経路情報の置き換え例を示す図である。

【図7】第2の実施形態によるルータに備えられる不正アクセス防止装置の動作を示すフローチャートである。

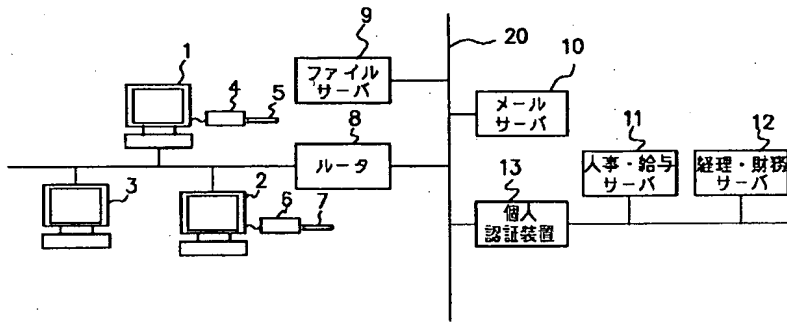
【図8】従来のネットワークシステム全体の構成を示す図である。

【符号の説明】

- 1, 2, 3 端末(パーソナルコンピュータ)
- 4, 6 専用リーダー
- 5, 7 ICカード
- 8 ルータ
- 9 ファイルサーバ
- 10 メールサーバ
- 11 人事・給与サーバ
- 12 経理・財務サーバ
- 13 個人認証装置
- 21 通信部
- 22 認証処理部
- 23 判断部
- 24 制御部
- 25 不正アクセス防止装置
- 31 通信部
- 32 判断部
- 33 制御部
- 34 不正アクセス防止装置
- 35 経路情報メモリ
- 36 退避メモリ

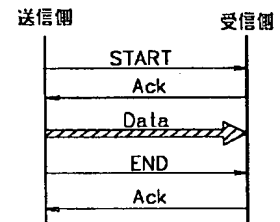
【図1】

ネットワークシステムの構成例



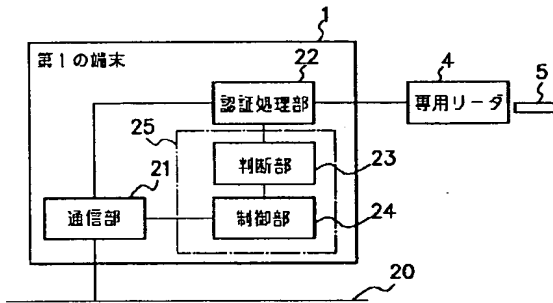
【図3】

通信のプロトコル



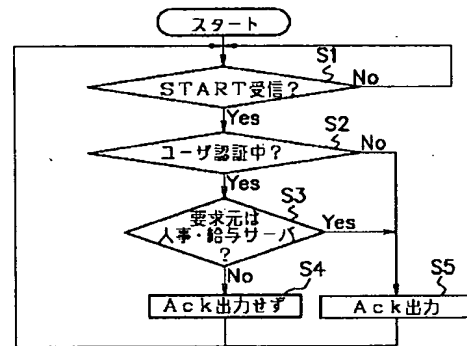
【図2】

第1の端末の機能構成例



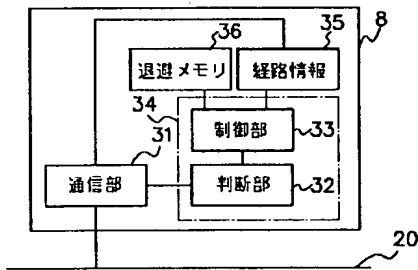
【図4】

第1の実施形態による動作フロー



【図5】

ルータの機能構成例



【図6】

経路情報の置換例

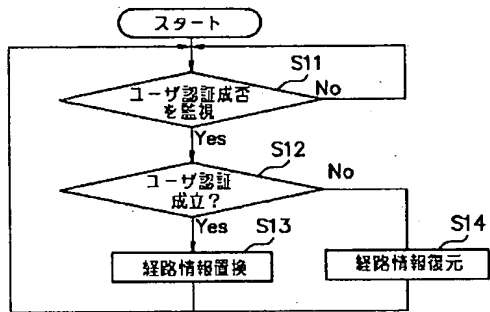
受信 発信	端末1	端末2	端末3	ファイル	メール	人・給	経・財	端末1
端末1	○	○	○	○	○	○	○	○
端末2	○	○	○	○	○	○	○	×
端末3	○	○	○	○	○	○	○	×
ファイル	○	○	○	○	○	○	○	×
メール	○	○	○	○	○	○	○	×
人・給	○	○	○	○	○	○	○	×
経・財	○	○	○	○	○	○	○	×

(a)

(b)

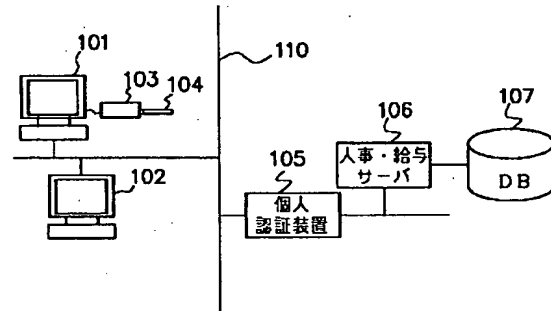
【図7】

第2の実施形態による動作フロー



【図8】

従来のネットワークシステム



フロントページの続き

Fターム(参考) 5B085 AE23 BG06  
 5J104 AA26 PA07  
 5K030 GA15 HA08 HC01 HC13 JT03  
 KA06 KA07 KA08 LA02 LC13

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-312316

(43)Date of publication of application : 25.10.2002

---

(51)Int.Cl. G06F 15/00

G06F 13/00

G09C 1/00

H04L 9/32

H04L 12/22

---

(21)Application number : 2001-114891 (71)Applicant : SUMISHO

COMPUTER SYSTEMS CORP

(22)Date of filing : 13.04.2001 (72)Inventor : KATO MICHIAKI

---

(54) UNLAWFUL COMPUTER ACCESS PREVENTION DEVICE AND  
METHOD, UNLAWFUL COMPUTER ACCESS PREVENTION PROGRAM AND  
RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To effectively prevent an unlawful computer access carried out by another person who successfully impersonates a correct user using a terminal in which a user certification is effected as a step.

SOLUTION: A judgment part 23 for judging whether or not the user certification is effected regarding a first terminal 1 connected onto a network 20 and a control part 24 for controlling it so as to disconnect an access from the outside to the first terminal 1 for the time when the user certification is effected (for example, a response is not returned even if an access requirement is sent to the first terminal 1 from the outside) are provided. The first terminal 1 cannot be hacked by disappearing the first terminal 1 in which the user certification is effected from

the outside. Thereby, it is effectively prevented that another person successfully impersonates the correct user using the first terminal 1 in which the user certification is effected as a step and unlawful computer accesses to the desired system.

---

LEGAL STATUS [Date of request for examination] 13.02.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

**\* NOTICES \***

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.

2. \*\*\*\* shows the word which can not be translated.

3. In the drawings, any words are not translated.

---

**CLAIMS**

---

[Claim(s)]

[Claim 1] The unlawful access arrester characterized by to have the control means controlled to intercept access from the outside to the above-mentioned terminal when it is judged that the above-mentioned user authentication has been materialized with a decision means judge whether user authentication required to access the system on the above-mentioned network or the above-mentioned network has been materialized about the terminal connected on the network, and the above-mentioned decision means.

[Claim 2] It is the unlawful access arrester applied to the terminal equipped with the function to receive user authentication required to access the system on a network or the above-mentioned network. When the access request has been sent to the above-mentioned terminal from the exterior through the

above-mentioned network. A decision means to judge whether the above-mentioned user authentication is materialized about the above-mentioned terminal. The unlawful access arrester characterized by having the control means controlled not to output the response to the above-mentioned access request when it is judged that the above-mentioned user authentication is materialized with the above-mentioned decision means.

[Claim 3] The above-mentioned control means is an unlawful access arrester according to claim 2 characterized by controlling not to output the response to the above-mentioned access request when the access request has been sent to the above-mentioned terminal through the above-mentioned network from the exteriors other than the system by which access was permitted by the above-mentioned user authentication while the above-mentioned user authentication is materialized about the above-mentioned terminal.

[Claim 4] It is the unlawful access arrester applied to the junction device on the network equipped with the function which judges and carries out data transfer of the following node transmitted with reference to path information based on a destination address. It is related with the terminal equipped with the function to receive user authentication required to access the system on the above-mentioned network or the above-mentioned network. When it is judged that the above-mentioned user authentication was materialized with a decision



means to judge whether the above-mentioned user authentication was materialized, and the above-mentioned decision means While transposing to the 2nd path information which intercepted the path which makes the destination the terminal with which the above-mentioned path information was evacuated and the above-mentioned user authentication was materialized The unlawful access arrester characterized by having the control means controlled to return the path information on the above 2nd to the path information on the origin which carried out [ above-mentioned ] evacuation when it is judged that the above-mentioned user authentication was canceled by the above-mentioned decision means.

[Claim 5] The path information on the above 2nd is an unlawful access arrester according to claim 4 characterized by being the path information for intercepting the path which made the above-mentioned terminal the destination from the exteriors other than the system by which access was permitted by the above-mentioned user authentication.

[Claim 6] When the access request has been sent to the terminal equipped with the function to receive user authentication required to access the system on a network or the above-mentioned network, through the above-mentioned network from the exterior The 1st step which judges whether the above-mentioned user authentication is materialized about the above-mentioned terminal, The unlawful access prevention approach characterized by having the 2nd step controlled not

to output the response to the above-mentioned access request when it is judged that the above-mentioned user authentication is materialized about the above-mentioned terminal.

[Claim 7] The unlawful access prevention approach according to claim 6 characterized by controlling by the 2nd step of the above not to output the response to the above-mentioned access request when the access request has been sent to the above-mentioned terminal through the above-mentioned network from the exteriors other than the system by which access was permitted by the above-mentioned user authentication while the above-mentioned user authentication is materialized about the above-mentioned terminal.

[Claim 8] It is related with the terminal equipped with the function to receive user authentication required to access the system on a network or the above-mentioned network. The 1st step which judges the success or failure of the above-mentioned user authentication, and when the above-mentioned user authentication is materialized about the above-mentioned terminal The 2nd step replaced with the 2nd path information which intercepted the path which makes the destination the terminal with which the above-mentioned path information of the data transfer junction [ / path information ] device to the following node based on a destination address was evacuated, and the above-mentioned user authentication was materialized, The unlawful access prevention approach

characterized by having the 3rd step which returns the path information on the above 2nd to the path information on the origin which carried out [ above-mentioned ] evacuation when the above-mentioned user authentication is canceled about the above-mentioned terminal.

[Claim 9] The path information on the above 2nd is the unlawful access prevention approach according to claim 8 characterized by being the path information for intercepting the path which made the above-mentioned terminal the destination from the exteriors other than the system by which access was permitted by the above-mentioned user authentication.

[Claim 10] The unlawful access prevention program for operating a computer as a control means which controls to intercept access from the outside to the above-mentioned terminal, when it is judged that the above-mentioned user authentication has been materialized with a decision means judge whether user authentication required to access the system on the above-mentioned network or the above-mentioned network has been materialized about the terminal connected on the network, and the above-mentioned decision means.

[Claim 11] When the access request has been sent to the terminal equipped with the function to receive user authentication required to access the system on a network or the above-mentioned network, through the above-mentioned network from the exterior A decision means to judge whether the above-mentioned user

authentication is materialized about the above-mentioned terminal, And the unlawful access prevention program for operating a computer as a control means controlled not to output the response to the above-mentioned access request, when it is judged that the above-mentioned user authentication is materialized with the above-mentioned decision means.

[Claim 12] It is related with the terminal equipped with the function to receive user authentication required to access the system on a network or the above-mentioned network. When it is judged that the above-mentioned user authentication was materialized with the decision means and the above-mentioned decision means of judging whether the above-mentioned user authentication having been materialized The above-mentioned path information of the data transfer junction [ / path information ] device to the following node based on a destination address is evacuated. When it is judged that the above-mentioned user authentication was canceled by the means replaced with the 2nd path information which intercepted the path which makes the destination the terminal with which the above-mentioned user authentication was materialized, and the above-mentioned decision means The unlawful access prevention program for operating a computer as a means to return the path information on the above 2nd to the path information on the origin which carried out [ above-mentioned ] evacuation.

[Claim 13] The record medium which is characterized by recording the program for operating a computer as each means of a publication on any 1 term of claims 10-12 and in which computer reading is possible.

---

## DETAILED DESCRIPTION

---

### [Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention is applied to the junction device on the terminal equipped with the function to receive user authentication required to access the system on a network or the network concerned, and the network equipped with the function which judges and carries out data transfer of the following node transmitted with reference to path information based on a destination address, concerning an unlawful access arrester and an approach, the program for unlawful access prevention, and a record medium, and is suitable.

[0002]

[Description of the Prior Art] In recent years, the information system using networks, such as the Internet and intranet, is used widely. In this information

system, it has been an important technical problem how the unauthorized entry by others, an information leak, an alteration, operation active jamming of the information system itself, etc. are prevented. Although some techniques exist as a security system for keeping the insurance of an information system, a user authentication technique is in one of them.

[0003] The typical thing of a user authentication technique is a password. That is, each user enters from a keyboard etc. the password of a proper assigned to itself, and if the password is collated by the personal authentication system and the right thing is confirmed, it comes to be able to perform access to the system on a network or the system concerned.

[0004] However, a hacking technique improves in recent years and it is becoming easy to steal a password. Therefore, in user authentication with a password, it was impossible to have prevented unlawful access by others completely as a matter of fact. So, recently, the user authentication technique with which decode used the difficult IC card is also used increasingly. However, even if it used this IC card, after that IC card itself was stolen, there was a possibility of others having become a normal user, having cleared up and accessing unjustly.

[0005] From such the actual condition, recently, the so-called biometric-person-authentication technique of identifying an individual, especially

using a fingerprint, voice, a face, etc. attracts attention, and is developed. Moreover, the technique which combined this and an IC card is also developed. for example, a user's fingerprint data -- an IC card -- storing -- network utilization time -- the IC card -- a terminal -- inserting -- a user -- his fingerprint data are collated, and if right, access to a network etc. will be permitted.

[0006]

[Problem(s) to be Solved by the Invention] According to an above-mentioned biometric-person-authentication technique, the user authentication technique which combined this and an IC card, compared with the case where a conventional password and a conventional IC card are used alone, it is possible to raise the safety of an information system. However, however it might make full use of a user authentication technique, when the terminal with which user authentication was materialized was hacked, the terminal was made a steppingstone and there was a problem that unjust access by others will be performed.

[0007] This is explained in detail using drawing 8 . In the system shown in drawing 8 , the 1st and 2nd terminal 101,102, and personnel affairs and a salary server 106 are connected through the network 110. The database 107 is connected to personnel affairs and the salary server 106, and the various data about personnel affairs and a salary are stored. In these various data, the

individual humanity news about individual school education, punishment, clinical recording, health condition, salary, etc. is also contained.

[0008] Personal authentication equipment 105 is installed between the 1st and 2nd terminal 101,102, and personnel affairs and a salary server 106. That it should avoid un-arranging [ that the data on a database 107 are altered or individual humanity news is stolen ], personal authentication equipment 105 performs processing about user authentication, in order to permit access to personnel affairs and the salary server 106 only to a specific user.

[0009] The exclusive reader 103 of IC card 104 is connected to the 1st terminal 101. The authentication information (biotechnology information, such as a user's status information or a fingerprint etc.) about the user who has an access privilege to personnel affairs and the salary server 106 is stored in IC card 104.

[0010] When the user of the 1st terminal 101 accesses personnel affairs and the salary server 106 through a network 110, IC card 104 is inserted in the exclusive reader 103, and the 1st terminal 101 is made to read one's authentication information first. The 1st terminal 101 sends the read authentication information to personal authentication equipment 105. Personal authentication equipment 105 checks the authentication information sent from the 1st terminal 101, and if right, it will permit access to personnel affairs and the salary server 106.

[0011] Thus, if user authentication is materialized to the 1st terminal 101, the



pass from the 1st terminal 101 concerned to personnel affairs and the salary server 106 through personal authentication equipment 105 will be formed. In this condition, if the 1st terminal 101 is hacked from the 2nd terminal 102, the 1st terminal 101 will be made a steppingstone and the user of the 2nd terminal 102 will be possible [ accessing unjustly at spoofing and personnel affairs and a salary server 106 at the user of the 1st terminal 1 ].

[0012] Thus, it is becoming difficult conventionally for amelioration to be added and, as for the user authentication technique itself, for others other than a normal user to receive user authentication. However, by hacking the terminal to which user authentication was materialized by the normal user, the terminal concerned will be made a steppingstone and it will enable them for others to become a normal user and to clear up. Therefore, unlawful access by others to the system on a network or the network concerned was not able to be prevented completely.

[0013] This invention is accomplished in order to solve such a problem, makes a steppingstone the terminal with which user authentication was materialized, and aims at enabling it to prevent effectively unlawful access that others become a normal user and clear up.

[0014]

[Means for Solving the Problem] The unlawful access arrester of this invention is

characterized by to have the control means controlled to intercept access from the outside to the above-mentioned terminal, when it is judged that the above-mentioned user authentication has been materialized with a decision means judge whether user authentication required to access the system on the above-mentioned network or the above-mentioned network has been materialized about the terminal connected on the network, and the above-mentioned decision means.

[0015] It is the unlawful access arrester applied to the terminal equipped with the function to receive user authentication required in other modes of this invention to access the system on a network or the above-mentioned network. When the access request has been sent to the above-mentioned terminal from the exterior through the above-mentioned network It is characterized by having a decision means to judge whether the above-mentioned user authentication is materialized about the above-mentioned terminal, and the control means controlled not to output the response to the above-mentioned access request when it is judged that the above-mentioned user authentication is materialized with the above-mentioned decision means.

[0016] In the mode of others of this invention, the above-mentioned control means is characterized by controlling not to output the response to the above-mentioned access request, when the access request has been sent to the

above-mentioned terminal through the above-mentioned network from the exteriors other than the system by which access was permitted by the above-mentioned user authentication while the above-mentioned user authentication is materialized about the above-mentioned terminal.

[0017] In the mode of others of this invention, path information is referred to based on a destination address. It is the unlawful access arrester applied to the junction device on the network equipped with the function which judges and carries out data transfer of the following node to transmit. It is related with the terminal equipped with the function to receive user authentication required to access the system on the above-mentioned network or the above-mentioned network. When it is judged that the above-mentioned user authentication was materialized with a decision means to judge whether the above-mentioned user authentication was materialized, and the above-mentioned decision means While transposing to the 2nd path information which intercepted the path which makes the destination the terminal with which the above-mentioned path information was evacuated and the above-mentioned user authentication was materialized When it is judged that the above-mentioned user authentication was canceled by the above-mentioned decision means, it is characterized by having the control means controlled to return the path information on the above 2nd to the path information on the origin which carried out [ above-mentioned ]

evacuation.

[0018] In the mode of others of this invention, path information on the above 2nd is characterized by being the path information for intercepting the path which made the above-mentioned terminal the destination from the exteriors other than the system by which access was permitted by the above-mentioned user authentication.

[0019] Moreover, when the access request has been sent to the terminal equipped with the function to receive user authentication required to access the system on a network or the above-mentioned network, through the above-mentioned network from the exterior, the unlawful access prevention approach of this invention It is characterized by having the 1st step which judges whether the above-mentioned user authentication is materialized about the above-mentioned terminal, and the 2nd step controlled not to output the response to the above-mentioned access request when it is judged that the above-mentioned user authentication is materialized about the above-mentioned terminal.

[0020] In other modes of this invention, at the 2nd step of the above, when the access request has been sent to the above-mentioned terminal through the above-mentioned network from the exteriors other than the system by which access was permitted by the above-mentioned user authentication while the

above-mentioned user authentication is materialized about the above-mentioned terminal, it is characterized by controlling not to output the response to the above-mentioned access request.

[0021] It is related with the terminal equipped with the function to receive user authentication required in the mode of others of this invention to access the system on a network or the above-mentioned network. The 1st step which judges the success or failure of the above-mentioned user authentication, and when the above-mentioned user authentication is materialized about the above-mentioned terminal The 2nd step replaced with the 2nd path information which intercepted the path which makes the destination the terminal with which the above-mentioned path information of the data transfer junction [ / path information ] device to the following node based on a destination address was evacuated, and the above-mentioned user authentication was materialized, When the above-mentioned user authentication is canceled about the above-mentioned terminal, it is characterized by having the 3rd step which returns the path information on the above 2nd to the path information on the origin which carried out [ above-mentioned ] evacuation.

[0022] In the mode of others of this invention, path information on the above 2nd is characterized by being the path information for intercepting the path which made the above-mentioned terminal the destination from the exteriors other than

the system by which access was permitted by the above-mentioned user authentication.

[0023] Moreover, the unlawful access prevention program of this invention is for operating a computer as a control means which controls to intercept access from the outside to the above-mentioned terminal, when it is judged that the above-mentioned user authentication has been materialized with a decision means judge whether user authentication required to access the system on the above-mentioned network or the above-mentioned network has been materialized about the terminal connected on the network, and the above-mentioned decision means.

[0024] When the access request has been sent to the terminal equipped with the function to receive user authentication required in other modes of this invention to access the system on a network or the above-mentioned network, through the above-mentioned network from the exterior A decision means to judge whether the above-mentioned user authentication is materialized about the above-mentioned terminal, And when it is judged that the above-mentioned user authentication is materialized with the above-mentioned decision means, it is characterized by operating a computer as a control means controlled not to output the response to the above-mentioned access request.

[0025] It is related with the terminal equipped with the function to receive user

authentication required in the mode of others of this invention to access the system on a network or the above-mentioned network. When it is judged that the above-mentioned user authentication was materialized with the decision means and the above-mentioned decision means of judging whether the above-mentioned user authentication having been materialized The above-mentioned path information of the data transfer junction [ / path information ] device to the following node based on a destination address is evacuated. When it is judged that the above-mentioned user authentication was canceled by the means replaced with the 2nd path information which intercepted the path which makes the destination the terminal with which the above-mentioned user authentication was materialized, and the above-mentioned decision means It is characterized by operating a computer as a means to return the path information on the above 2nd to the path information on the origin which carried out [ above-mentioned ] evacuation.

[0026] Moreover, the record medium which can computer read this invention is characterized by recording the program for operating a computer as each means of a publication on any 1 term of claims 10-12.

[0027]

[Embodiment of the Invention] (1st operation gestalt) The 1st operation gestalt of this invention is hereafter explained based on a drawing. Drawing 1 is drawing

showing the configuration of the whole network system which applied the unlawful access arrester by this operation gestalt.

[0028] In drawing 1 , personnel affairs and a salary server, and 12 are connected so that a file server and 10 may be accounting and a financial server a mail server and 11 and, as for the terminal with which 1, 2, and 3 consist of a personal computer etc., and 9, these can communicate mutually through a network 20.

[0029] A file server 9 processes transfer of a file, deletion, directory actuation, etc. A mail server 10 performs processing handed over when the electronic mail was transmitted, or the delivered electronic mail is kept and there is enquiry from terminals 1, 2, and 3 based on the demand from terminals 1, 2, and 3. Personnel affairs and the salary server 11 perform various processings about the personnel affairs and the salary in a company. Accounting and the financial server 12 perform various processings about the accounting and financial affairs in a company. In addition, since these various servers 9-12 can use a well-known thing, detailed explanation of the contents of processing is omitted here.

[0030] 8 is a router and is installed in the suitable location on a network 20. The data transmitted on the network 20 from a certain computer are surely sent to the target computer via a router 8. This router 8 judges the following node to transmit based on the destination IP address in IP header with reference to the



path information (routing table) which router 8 self has, and transmits data.

[0031] 13 is personal authentication equipment and is installed between the 1st - the 3rd terminal 1-3, and personnel affairs, the salary server 11 and accounting and a financial server 12. Personal authentication equipment 13 performs processing about user authentication based on the authentication information sent from the 1st and 2nd terminals 1 and 2, in order to permit access to personnel affairs and the salary server 11, and accounting and a financial server 12 only to a specific user.

[0032] The exclusive reader 4 of IC card 5 is connected to the 1st terminal 1. The authentication information (biotechnology information, such as a user's status information or a fingerprint etc.) about the user who has an access privilege to personnel affairs and the salary server 11 is stored in IC card 5. The user of the 1st terminal 1 can also access personnel affairs and the salary server 11 by receiving user authentication using IC card 5 while being able to access a file server 9 and a mail server 10 freely.

[0033] When the user of the 1st terminal 1 accesses personnel affairs and the salary server 11, IC card 5 is inserted in the exclusive reader 4, and the 1st terminal 1 is made to read one's authentication information first. The 1st terminal 1 sends the read authentication information to personal authentication equipment 13 through a router 8. Personal authentication equipment 13 checks

the authentication information sent from the 1st terminal 1, and if right, it will permit access to personnel affairs and the salary server 11.

[0034] Moreover, the exclusive reader 6 of IC card 7 is connected to the 2nd terminal 2. The authentication information (biotechnology information, such as a user's status information or a fingerprint etc.) about the user who has an access privilege to accounting and the financial server 12 is stored in IC card 7. The user of the 2nd terminal 2 can also access accounting and the financial server 12 by receiving user authentication using IC card 7 while being able to access a file server 9 and a mail server 10 freely.

[0035] When the user of the 2nd terminal 2 accesses accounting and the financial server 12, IC card 7 is inserted in the exclusive reader 6, and the 2nd terminal 2 is made to read one's authentication information first. The 2nd terminal 2 sends the read authentication information to personal authentication equipment 13 through a router 8. Personal authentication equipment 13 checks the authentication information sent from the 2nd terminal 2, and if right, it will permit access to accounting and the financial server 12.

[0036] The 3rd terminal 3 is not equipped with the function for receiving user authentication. That is, it does not have an access privilege to personnel affairs, the salary server 11, and accounting and a financial server 12, but the user of the 3rd terminal 3 can be accessed only to a file server 9 and a mail server 10.

[0037] In addition, although considered as the configuration which forms the exclusive readers 4 and 6 of IC cards 5 and 7 by external [ of the 1st and 2nd terminals 1 and 2 ] here, the 1st and 2nd terminals 1 and 2 the very thing may be equipped with the reading function of IC cards 5 and 7. Moreover, although IC cards 5 and 7 are used in order to receive user authentication here, this invention does not limit especially the approach of user authentication. For example, other user authentication techniques, such as a password, may be used.

[0038] Moreover, although what needs user authentication for accessing was made into personnel affairs, the salary server 11, and accounting and a financial server 12, it is not limited to these servers here. For example, it may be made to consider as the prerequisite of access to the user authentication by personal authentication equipment 13 also with other servers or file servers 9 which are not illustrated, a mail server 10, or the host computer which is not illustrated.

[0039] Drawing 2 is the block diagram showing the example of a functional configuration of the 1st terminal 1. In addition, since it is constituted like [ the 2nd terminal 2 ] the 1st terminal 1, illustration is omitted here. In drawing 2, 21 is the communications department and performs processing about transmission and reception of data through a network 20. 22 is the authentication processing section, moves together with personal authentication equipment 13, and

performs processing about user authentication.

[0040] The above-mentioned authentication processing section 22 incorporates the authentication information in IC card 5 read by the exclusive reader 4, and has the function transmitted to personal authentication equipment 13 through the communications department 21. Moreover, the authentication authorization information sent through the communications department 21 from personal authentication equipment 13 is incorporated, and it also has the function to hold. Only while the authentication processing section 22 holds authentication authorization information, it is possible to access personnel affairs and the salary server 11.

[0041] 23 is the decision section, and when the access request has been sent to the communications department 21 through a network 20 from the exterior, it judges whether user authentication is materialized about the 1st terminal 1 by seeing authentication authorization information whether held by the authentication processing section 22.

[0042] In addition, although authentication authorization information is made to hold in the authentication processing section 22 here and the success or failure of user authentication are judged by the existence of the information concerned, this invention is not limited to this example. For example, when the access request has been sent from the exterior, you may make it ask personal

authentication equipment 13 the success or failure of user authentication through the communications department 21. In this case, personal authentication equipment 13 will hold authentication authorization information.

[0043] 24 is a control section, and when the access request has been sent to the 1st terminal 1 through a network 20 from the exterior while user authentication is materialized about the 1st terminal 1, it is controlled not to output the response to the access request from the communications department 21. On the other hand, when user authentication is not materialized about the 1st terminal 1, it usually passes and controls to output a response to the access request from the outside.

[0044] The unlawful access arrester 25 of this operation gestalt is constituted by the above-mentioned decision section 23 and the control section 24. This unlawful access arrester 25 consists of a CPU of the 1st terminal 1, MPU, RAM, ROM, etc. in fact, and the functional configuration of the decision section 23 and the control section 24 which were mentioned above when the program memorized by RAM and ROM operated is realized.

[0045] Therefore, the program operated so that the 1st terminal 1 may achieve the function of the above-mentioned decision section 23 and a control section 24 is recorded on a record medium like CD-ROM, and it can realize by making it read into a computer. As a record medium which records the above-mentioned program, a floppy (trademark) disk, a hard disk, a magnetic tape, an optical disk,

a magneto-optic disk, DVD, a non-volatile memory card, etc. can be used in addition to CD-ROM. Moreover, you may make it download the above-mentioned program from other computers through a network 20.

[0046] moreover, the function of the decision section 23 and a control section 24 is not only realized by performing the program to which the 1st terminal 1 was supplied, but The case where an above-mentioned function is realized in collaboration with OS (operating system) or other application software etc. with which the program is working in the 1st terminal 1, Also when all or a part of supplied processing of a program is performed by the 1st functional add-in board and functional expansion unit of a terminal 1 and an above-mentioned function is realized, this program is included in the operation gestalt of this invention.

[0047] Drawing 3 is drawing showing a general communications protocol. When transmitting data to a receiving side from a transmitting side, the signal START which tells starting data transmission is first sent to a receiving side from a transmitting side. If a reply signal Ack is returned to a transmitting side from a receiving side corresponding to this, Data Data will be sent to a receiving side from a transmitting side. Termination of data transmission sends the signal END which tells that data transmission was completed to a receiving side from a transmitting side. A series of data communication is completed by returning a reply signal Ack to a transmitting side from a receiving side corresponding to this.

[0048] In such a communications protocol, a control section 24 is controlled not to return the reply signal Ack over it, when the data transmitting start signal START which is an access request has been sent from the outside while user authentication is materialized about the 1st terminal 1. By doing in this way, the 1st terminal 1 becomes possible [ showing as it does not exist on a network 20 ] to access request origin.

[0049] Usually, hacking to the 1st terminal 1 with which user authentication is materialized sends temporary data to the 1st terminal 1 from the exterior, and is performed by checking the existence location on the network 20 of the 1st terminal 1. However, since a response is not returned to the access request from the outside while user authentication is materialized, the 1st terminal 1 existence of the 1st terminal 1, and it becomes impossible [ the terminal ] according to this operation gestalt entirely to access the 1st terminal 1. [ exterior ]

[0050] It completely becomes impossible to hack the 1st terminal 1 with which it followed, for example, user authentication was materialized from the 3rd terminal 3, it can make the 1st terminal 1 a steppingstone, and can prevent effectively unlawful access to the personnel affairs and the salary server 11 by others becoming the user of the 1st terminal 1 and clearing up. Unlawful access to the accounting and the financial server 12 which it also becomes impossible similarly to have hacked the 2nd terminal 2 with which user authentication was

materialized, and made the 2nd terminal 2 a steppingstone can also be prevented effectively.

[0051] Although it is possible to access personnel affairs and the salary server 11 from the 1st terminal 1 while user authentication is materialized, for example about the 1st terminal 1, it becomes impossible to access the 1st terminal 1 from personnel affairs and the salary server 11 conversely in the above example. However, a timer is set to Nighttime, for example and demand of printing by starting from personnel affairs and the salary server 11, and sending desired data to the 1st terminal 1 also exists.

[0052] Since it corresponds to such a demand, also while user authentication is materialized about the 1st terminal 1, the thing to which a permission is granted and which is made like (a reply signal Ack is returned) is also possible only for access from the personnel affairs and the salary server 11 to which access was permitted by user authentication. That is, the control section 24 in this case is controlled not to output the response to that access request, when the access request has been sent to the 1st terminal 1 through a network 20 from computers personnel affairs and other than salary server 11.

[0053] Drawing 4 is a flow chart which shows actuation of the unlawful access arrester 25 with which the 1st terminal 1 in this case is equipped. In drawing 4, a control section 24 judges whether user authentication is materialized about the



1st terminal 1 of the present using the decision section 23, when the communications department 21 supervises whether the data transmitting start signal START was received from the exterior (step S1) and receives this (step S2).

[0054] When current user authentication is not materialized, even if the 1st terminal 1 is hacked, since it is impossible, making the 1st terminal 1 concerned a steppingstone and accessing personnel affairs and the salary server 11 will control the communications department 21 to usually pass and to return a reply signal Ack (step S5). This becomes possible to access freely from the outside to the 1st terminal 1.

[0055] On the other hand, when current user authentication is materialized, a control section 24 judges whether access request origin (data transmitting start signal START dispatch-origin) is personnel affairs and the salary server 11 (step S3). When performing user authentication using IC card 5 like this operation gestalt and setting authentication information as the IC card 5, the IP address of personnel affairs and the salary server 11 is also held. Therefore, it is possible to judge whether access request origin is personnel affairs and the salary server 11 by obtaining whether the IP address read in IC card 5 and the IP address sent with the data transmitting start signal START are in agreement.

[0056] When access request origin is not personnel affairs and the salary server

11, a control section 24 controls the communications department 21 not to return a reply signal Ack to the data transmitting start signal START (step S4). Thereby, it is made for the 1st terminal 1 not to appear from the outside, and unlawful access to the personnel affairs and the salary server 11 which made the 1st terminal 1 a steppingstone is prevented.

[0057] Moreover, when access request origin is personnel affairs and the salary server 11, a control section 24 controls the communications department 21 to return a reply signal Ack to the data transmitting start signal START (step S5). This becomes possible to access to personnel affairs and the salary server 11 freely to the 1st terminal 1.

[0058] Since it is controlling in the 1st operation gestalt to intercept access from the outside to these terminals 1 and 2 while user authentication is materialized about the 1st and 2nd terminals 1 and 2 as explained in detail above, it can avoid hacking the 1st and 2nd terminals 1 and 2. By this, the 1st and 2nd terminals 1 and 2 can be made a steppingstone, others can pass personal authentication equipment 13, and it can prevent effectively accessing unjustly personnel affairs and the salary server 11, accounting, a financial server 12, etc.

[0059] (2nd operation gestalt) Next, the 2nd operation gestalt of this invention is explained based on a drawing. The configuration of the whole network system which applied the unlawful access arrester by the 2nd operation gestalt is the

same as that of drawing 1 . However, the 1st and 2nd terminals 1 and 2 are not equipped with the functional configuration of the unlawful access arrester 25 shown in drawing 2 . In this operation gestalt, an unlawful access arrester is formed in a router 8.

[0060] Drawing 5 is the block diagram showing the example of a functional configuration of a router 8. In drawing 5 , 31 is the communications department and performs processing about data transfer through a network 20. That is, with reference to the path information (routing table) currently held at the path information memory 35, the following node to transmit is judged based on the destination IP address in IP header of the data sent through a network 20, and data are transmitted.

[0061] 32 is the decision section and judges the success or failure of the user authentication about the 1st terminal 1 and 2nd terminal 2. When the 1st and 2nd terminals 1 and 2 receive user authentication, data required for user authentication are exchanged via a router 8 among these terminals 1 and 2 and personal authentication equipment 13. Therefore, when the decision section 32 supervises the data which mind the communications department 31 of a router 8 in the case of activation of user authentication, and are carried out at it, it is possible to check that user authentication was materialized or that user authentication has been canceled after that.

[0062] In addition, the technique of judging the success or failure of the user authentication about the 1st and 2nd terminals 1 and 2 is not limited to this. For example, when user authentication is materialized or canceled by the 1st and 2nd terminals 1 and 2, you may make it tell that clearly to a router 8 from the 1st and 2nd terminals 1 and 2.

[0063] 33 is a control section, when it is judged that user authentication was materialized about the 1st terminal 1 or 2nd terminal 2 by the decision section 32, evacuates the path information in the path information memory 35 to the evacuation memory 36, and transposes the contents of the path information memory 35 to the 2nd path information which intercepted the path which makes the destination the terminal with which user authentication was materialized. Moreover, when it is judged that user authentication was canceled, it controls to return the path information on the origin which evacuated to the evacuation memory 36 to the path information memory 35.

[0064] The unlawful access arrester 34 of this operation gestalt is constituted by the above-mentioned decision section 32 and the control section 33. This unlawful access arrester 34 consists of a CPU of a router 8, MPU, RAM, ROM, etc. in fact, and the functional configuration of the decision section 32 and the control section 33 which were mentioned above when the program memorized by RAM and ROM operated is realized.

[0065] Drawing 6 is drawing showing the example of replacement of path information. Drawing 6 (a) shows in image the path information (routing table) memorized from the first by the path information memory 35. O mark in a table shows that a path exists. Usually, all the paths about each node connected on the network 20 serve as O mark.

[0066] In addition, from the 1st terminal 1, being written as "IC" in the path over accounting and the financial server 12 from the path and the 2nd terminal 2 over personnel affairs and the salary server 11 shows that it is the path to which access is permitted, when user authentication is received using IC cards 5 and 7. Moreover, although the path over personnel affairs and the salary server 11, or accounting and a financial server 12 also serves as O mark from other nodes, it does not mean that this only shows that there is only such a path, and has permitted access.

[0067] For example, suppose that user authentication was materialized about the 1st terminal 1. In this case, the path information on a part that the 1st terminal 1 serves as a receiving side is replaced like drawing 6 (b). x mark in drawing 6 (b) means that such a path does not exist. This replacement is equivalent to canceling all the path information from other nodes to the 1st terminal 1. When carrying out this replacement, in order to enable it to restore the path information on original later, the path information before replacing is

evacuated to the evacuation memory 36.

[0068] Then, if IC card 5 is extracted in the 1st terminal 1 and user authentication is canceled, the condition of drawing 6 (a) will be restored by returning the path information on the origin which evacuated to the evacuation memory 36 to the path information memory 35. In addition, the path information evacuated to the evacuation memory 36 at the time of formation of user authentication may be all path information shown in drawing 6 (a), and may be only parts to replace.

[0069] Thus, while user authentication is materialized about the 1st terminal 1, the 1st terminal 1 becomes possible [ showing as it does not exist on a network 20 ] to access request origin by covering a mask over the path information on a path that it results [ from other nodes ] in the 1st terminal 1. Although it surely goes via a router 8 in case the 1st terminal 1 is accessed, since the path information in the router 8 is replaced at the time of user authentication formation, existence of the 1st terminal 1 cannot be known from the exterior, but it becomes impossible entirely to access the 1st terminal 1.

[0070] It completely becomes impossible to hack the 1st terminal 1 with which it followed, for example, user authentication was materialized from the 3rd terminal 3, it can make the 1st terminal 1 a steppingstone, and can prevent effectively unlawful access to the personnel affairs and the salary server 11 by others becoming the user of the 1st terminal 1 and clearing up. Unlawful access to the

accounting and the financial server 12 which it also becomes impossible similarly to have hacked the 2nd terminal 2 with which user authentication was materialized, and made the 2nd terminal 2 a steppingstone can also be prevented effectively.

[0071] In addition, also in the 2nd operation gestalt, also while user authentication is materialized, for example about the 1st terminal 1, the thing to which a permission is granted and which is made like (the mask of the path information on a path that it results [ from personnel affairs and the salary server 11 ] in the 1st terminal 1 is not carried out) is also possible only for access from the personnel affairs and the salary server 11 to which access was permitted by user authentication. That is, the 2nd part is considered as O mark from the bottom in the example of drawing 6 (b).

[0072] Drawing 7 is a flow chart which shows actuation of the unlawful access arrester 34 by the 2nd operation gestalt. In drawing 7 , the control section 33 in a router 8 is supervising the success or failure (formation and discharge of user authentication) of user authentication about the 1st terminal 1 and 2nd terminal 2 using the decision section 32 (step S11).

[0073] When user authentication is not materialized by the both sides of the 1st terminal 1 and the 2nd terminal 2, even if these terminals 1 and 2 are hacked, since it is impossible, making the terminals 1 and 2 concerned a steppingstone

and accessing them at personnel affairs and the salary server 11, or accounting and a financial server 12 will hold the usual path information as it is in the path information memory 35, and it will continue supervising the success or failure of user authentication. It is possible for this to access freely from the outside to the 1st terminal 1 and 2nd terminal 2.

[0074] When the success or failure of user authentication have change about the 1st terminal 1 or 2nd terminal 2, it judges whether it is formation of user authentication (step S12). When user authentication is materialized to the 1st terminal 1 or 2nd terminal 2, the path information about the terminal with which the user authentication was materialized is evacuated from the path information memory 35 to the evacuation memory 36, and the 2nd path information which carried out the mask of the path which results in the terminal concerned is transposed to the path information memory 35 (step S13).

[0075] On the other hand, when user authentication is canceled about the 1st terminal 1 or 2nd terminal 2, the path information about the terminal of which the user authentication was canceled is restored to the path information memory 35 from the evacuation memory 36 (step S14). After processing of the above-mentioned step S13 or step S14 returns to step S11, and continues the monitor of user authentication success or failure.

[0076] Since it is controlling also in the 2nd operation gestalt to intercept access



from the outside to these terminals 1 and 2 while user authentication is materialized about the 1st and 2nd terminals 1 and 2 as explained in detail above, it can avoid hacking the 1st and 2nd terminals 1 and 2. By this, the 1st and 2nd terminals 1 and 2 can be made a steppingstone, others can pass personal authentication equipment 13, and it can prevent effectively accessing unjustly personnel affairs and the salary server 11, accounting, a financial server 12, etc.

[0077] In addition, it passes over no each operation gestalten explained above to what showed an example of the somatization which hits carrying out this invention, and the technical range of this invention must not be restrictively interpreted by these. That is, this invention can be carried out in various forms, without deviating from the pneuma or its main description. For example, you may apply combining the 1st operation gestalt and the 2nd operation gestalt.

[0078]

[Effect of the Invention] Since this invention is controlled to intercept access from the outside to the terminal with which the user authentication was materialized while user authentication is materialized about the terminal connected on the network, as mentioned above, it can avoid hacking the terminal with which user authentication was materialized. It can prevent effectively others becoming to a normal user at a step, clearing up the terminal with which user authentication

was materialized, and accessing unjustly by this, at a target network and a target system.

---

## DESCRIPTION OF DRAWINGS

---

[Brief Description of the Drawings]

[Drawing 1] It is drawing showing the configuration of the whole network system which applied the unlawful access arrester by the 1st and 2nd operation gestalten.

[Drawing 2] It is the block diagram showing the example of a functional configuration of the 1st terminal by the 1st operation gestalt.

[Drawing 3] It is drawing showing a general communications protocol.

[Drawing 4] It is the flow chart which shows actuation of the unlawful access arrester with which the 1st terminal by the 1st operation gestalt is equipped.

[Drawing 5] It is the block diagram showing the example of a functional configuration of the router by the 2nd operation gestalt.

[Drawing 6] It is drawing showing the example of replacement of path information.

[Drawing 7] It is the flow chart which shows actuation of the unlawful access

arrester with which the router by the 2nd operation gestalt is equipped.

[Drawing 8] It is drawing showing the configuration of the conventional whole network system.

[Description of Notations]

1, 2, 3 Terminal (personal computer)

4 Six Exclusive reader

5 Seven IC card

8 Router

9 File Server

10 Mail Server

11 Personnel Affairs and Salary Server

12 Accounting and Financial Server

13 Personal Authentication Equipment

21 Communications Department

22 Authentication Processing Section

23 Decision Section

24 Control Section

25 Unlawful Access Arrester

31 Communications Department

32 Decision Section

33 Control Section

34 Unlawful Access Arrester

35 Path Information Memory

36 Evacuation Memory